coreboot - Bug #158

Skylake: SGX feature conflicts with VMX

02/09/2018 08:50 PM - Youness Alaoui

Status:	Resolved	**Start date:**	02/09/2018
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			

Description

If you enable SGX, it will cause the Features (MSR 0x3A: IA32_FEATURE_CONTROL) to be locked before the FSP SiliconInit runs, and that will prevent the FSP from enabling the VMX features.
If we set register 'SgxEnable' to 1 and set the 'PrmrrSize' in the devicetree, we can see this in the cbmem :

SGX activation was successful.
Calling FspSiliconInit: 0x6faec1da

Which shows SGX activation happening before FspSiliconInit. The sgx_configure in soc/intel/common/block/sgx/sgc. will call lock_sgx() which actually locks the entire IA32_FEATURE_CONTROL.
Doing a 'rdmsr -x 0x3a' shows an MSR result of 0x4001 which has SGX enabled and VMX disabled. If we remove the lock_sgx() then the FSP will reset the feature control (even if EnableSgx is set in the FSP-M UPD) and we end up with an MSR of 0x4 (VMX enabled but SGX disabled).
I think the best solution here is to enable SGX after the FSP has run. Also, is it worth making the Feature lock a configuration option ?

History

#1 - 05/28/2019 02:49 PM - Matt DeVillier

- Status changed from New to Resolved

this was resolved in f9aed6578565593ff2b5d9e90f8e6e80e5d9831d [cpu/intel/common: decouple IA32_FEATURE_CONTROL lock from set_vmx()]